Journal of *Marine Science and Engineering*

MDPI

Article

Enabling Future Maritime Traffic Management: A Decentralized Architecture for Sharing Data in the Maritime Domain

Dennis Höhn *, Lorenz Mumm, Benjamin Reitz, Christina Tsiroglou and Axel Hahn

German Aerospace Center (DLR), Institute of Systems Engineering for Future Mobility, Escherweg 2, 26121 Oldenburg, Germany; lorenz.mumm@dlr.de (L.M.); benjamin.reitz@dlr.de (B.R.); christina.tsiroglou@dlr.de (C.T.); axel.hahn@dlr.de (A.H.)

* Correspondence: dennis.hoehn@dlr.de

Abstract: Digitalization is transforming the maritime sector, and the amount and variety of data generated is increasing rapidly. Effective data utilization is crucial for data-driven services such as for highly automated maritime systems and efficient traffic coordination. However, these applications depend on heterogeneous, distributed data sources managed by different actors, making secure and sovereign information sharing difficult. This paper investigates how maritime data can be exchanged reliably and securely without jeopardizing data sovereignty. Based on the existing literature, we identify the main challenges and current research gap in sharing maritime information, emphasizing the importance of data availability. From this, we derive requirements for a secure and sovereign infrastructure for data exchange. To address these challenges, we propose a fully decentralized architecture for the maritime sector based on the concept of a data space. Our approach integrates protocols to improve data availability while minimizing data volume, considering maritime constraints such as volatile connectivity, low bandwidth and existing standards. We evaluate our architecture through a maritime traffic management case study and demonstrate its ability to enable secure and sovereign exchange of heterogeneous data. The results confirm that our solution reliably supports distributed data collection and enables data-driven, value-added services, which in turn will improve the safety and efficiency of the maritime domain in the near future.

Keywords: data management; maritime traffic management; data-driven services; Data Spaces; volatile connectivity; maritime standards

Academic Editors: Nikitas Nikitakos and Iosif Progoulakis

Received: 12 March 2025
Revised: 31 March 2025
Accepted: 2 April 2025
Published: 5 April 2025

Citation: Höhn, D.; Mumm, L.; Reitz, B.; Tsiroglou, C.; Hahn, A. Enabling Future Maritime Traffic Management: A Decentralized Architecture for Sharing Data in the Maritime Domain. *J. Mar. Sci. Eng.* **2025**, *13*, 732. https://doi.org/10.3390/jmse13040732

1. Introduction

Despite the enormous economic importance of the maritime domain for global trade and the advancing digitalization, maritime transport is surprisingly uncoordinated compared to other sectors such as aviation [1,2]. However, it should be noted that the coordination of individual actors can have a positive impact on traffic. Because of this, coordination safety can be increased, waiting times reduced and emissions lowered. In today's maritime shipping industry, each vessel decides locally how it wants to travel without having a holistic view of the overall situation [3]. In order to derive meaningful actions, a comprehensive picture of the situation is required, which shows, e.g., where other actors are currently located, which services will be available at the port at the time of arrival or how the weather conditions will change during the voyage [4]. All these parameters and much more contextual information help to get a better understanding of the current situation at sea and positively influence the planning of a voyage. An ideal solution therefore cannot be found locally on board a single vessel, as in practice the necessary information is simply not

available [5]. This in turn inevitably leads to unintentional planning errors and phenomena such as "hurry-up-and-wait" [2]. In so-called "hurry-up-and-wait", vessels compete to be the first to arrive at the port to be processed first. This behavior not only poses an increased safety risk but is also very inefficient as it leads to longer waiting times, increased emissions and inefficient use of port-resources [6].

To counteract this problem, a promising solution is emerging: the introduction of centralized traffic control, comparable to the concept of air traffic controllers in aviation [4,7]. The idea of the new approach is to create an instance that monitors the current traffic situation of an entire area and derives instructions for action, such as course or speed adjustments, to the individual traffic participants, so that the traffic is optimized overall with regard to definable target parameters such as emissions or waiting times [3,8]. Centralizing traffic management would make it possible to find a holistically optimal solution instead of many local, suboptimal partial solutions [8]. In addition, only one neutral body, such as the Vessel Traffic Service (VTS), would need to have a complete picture of the current situation to send optimized instructions to the individual actors [7]. However, decentralized approaches to maritime traffic management have also been discussed in the literature, in which the individual actors negotiate their instructions bilaterally or multilaterally [9].

Regardless of what the traffic management of the future will look like, all options have in common their reliance on a comprehensive situational picture [10]. In practice, creating a situation picture is also a challenge, as the information required for this is distributed across a variety of different maritime actors, such as shipping companies, weather services, ports, logistics companies, and many more [6]. All of these stakeholders pursue their own (sometimes conflicting) interests and have their own technical infrastructures with proprietary interfaces [11]. This in turn leads to great reluctance to share data with each other, as the stakeholders are either afraid of losing the control over their data-asset or the exchange would involve too much technical effort to align the interfaces of the various IT-systems [12]. The question therefore arises of how the required data can be exchanged in a standardized and secure way so that the associated technical effort and mistrust in providing external parties with data can be reduced to a minimum. In addition to the decentralized nature of the required information basis, volatile connections between sea- and land-based actors also pose a challenge when exchanging information [13]. The available bandwidth on the open sea varies from just a few kilobits per second to several megabits per second. However, currently available solutions have usually in common that they are charged per megabyte used. At around 00.20 to 19.32 USD per megabyte, the costs are very variable but still very significant, meaning that careful use makes sense economically [14,15]. In addition, despite global coverage, interrupted connections or high latency times (about 700 ms) must be expected all the time [16]. Thus, the optimization of maritime traffic requires not only an intelligent algorithm for planning but also a corresponding data infrastructure that makes it possible to obtain all relevant information to derive a meaningful picture of the current situation at open sea at any time [10].

Structure and Methology

Therefore, in this paper, we will present a new approach for a decentralized architecture that makes it feasible to share information in a secure and sovereign way for maritime actors, while taking maritime requirements, like volatile connections and standards, into account. In Section 2, we initially provide relevant background information regarding the current challenges in sharing data in the maritime domain and present promising approaches to realize a sovereign data exchange. On this basis, we subsequently derive requirements for a maritime data management system ensuring secure and reliable data exchange. Section 3 takes a closer look at the related work. It provides an insight into

ongoing cross-domain initiatives for sovereign information exchange as well as relevant existing projects and approaches for the realization of sovereign data exchange in the maritime sector. The related work is compared against the requirements identified in Section 2, on which basis the research gap for this paper is derived in a structured way. In Section 4, our architecture for a system that enables sovereign and secure data exchange in the maritime domain is presented in detail. Afterwards, in Section 5 the proposed architecture is practically evaluated using an application-oriented scenario from maritime traffic management. The results of the case study are discussed in detail in Section 6. Finally, Section 7 summarizes the obtained results and provides insight into limitations and future work.

2. Background

The following section outlines the current challenges that arise in the exchange of information, especially in the maritime domain. It also provides an insight into the concept of Data Spaces, which enables sovereign and trustworthy data sharing. Finally, the requirements for the architecture to be developed are derived based on the challenges and existing approaches.

2.1. Challenges in Sharing Data in the Maritime Domain

It is not only traffic optimization services that rely on the constant provision of information; collision avoidance and the automation of maritime traffic also require data that is as up to date and comprehensive as possible. The provision of a maritime service generally requires a comprehensive data basis that relies on a variety of heterogeneous data sources. This can include ship-related information such as the current draught, position, and load, harbor information such as planned docking and casting off times, as well as available berths and data on hinterland connections. In practice, these heterogeneous data sets are not collected by a single actor. The data are usually distributed across a large number of different stakeholders, each of which collects data on their central area of interest. For instance, a harbor has precise information on the available berths but does not necessarily collect data on the current traffic situation or weather conditions. However, in order for an actor to optimize its operational processes, it is therefore also directly dependent on further data from other actors that is as detailed and up to date as possible. For example, a port should be informed as early as possible about delays in the arrival of ships so that it can adjust its planning of available berths accordingly—which in turn can only be derived from a situation picture that exceeds the area of its own port and must therefore be queried from previous ports or from the responsible shipping company itself.

However, the acquisition of the required data is usually accompanied by four major challenges—the technical heterogeneity of IT-systems, an option for global secure authentication, the sovereign provision of data, and the management of maritime environmental conditions. These four challenges are described in detail in the following section:

1. **Technical heterogeneity of IT-systems**: Due to the global nature of the domain, there are several challenges to overcome when exchanging data. A key challenge when exchanging heterogeneous data is that the required information is provided by different companies, organizations, and authorities and their technical systems are not harmonized with each other [17]. Therefore, these systems generally do not have standardized and interoperable interfaces that are required for a seamless data exchange. If two parties are interested in exchanging data, they have to exchange data via their interfaces and find a customized way to link their two systems. This manual process is very time-consuming and therefore costly for both parties [18]. The unavailability of standardized interfaces therefore means that the individual

actors must first carefully weigh up whether it is worth the effort of adapting their systems for the planned data exchange. The increased costs can in turn lead to the maritime actors not exchanging their data with each other. In addition, the necessary preparatory work makes it impossible to transmit information between unknown parties at short notice, which is, e.g., essential for security and rescue operations [19].

2. **Global secure authentication of maritime actors**: Another challenge is the establishment of trust between actors. To exchange data, the actors have to trust each other to a certain degree [20]. For example, if a navigational warning is issued, the consumer of this information has to trust the issuing party that the warning is valid. Otherwise, they might ignore the warning and the consequences can be accidents or mishaps. Another example is the exchange of business-relevant data, for example, data of the Estimated Time of Arrival (ETA) from a vessel. The information could also be useful for competitors to adapt their own fleet planning to that of the competition. If such information is therefore exchanged with third parties, it must be ensured that only the intended recipient receives the information so that there is no loss of trust or economic damage.

What both scenarios have in common is that the parties involved must be able to authenticate themselves securely. In the physical world, we use ID cards or authenticated documents from a notary for this; these authentication methods cannot be used when transferring information. In the digital world, the concept of digital identities has proven itself in recent decades [21]. These digital identities are issued by so-called Identity Providers. An Identity Provider first checks in the real world whether the requesting actor is actually the entity or not, before issuing an identity. If the check is successful, a digital certificate is issued by the Identity Provider with which the actor can cryptographically authenticate itself to other actors [21]. The trust in the digital identities consists in the cryptographic security of the approach (forgery of a digital signature is almost impossible nowadays) and in the trust in the Identity Provider itself who issues the certificates. In particular, the second point poses a major challenge in the global maritime world, as it is almost impossible to find an entity that is trusted by all actors worldwide. There can be many reasons for this, for example, they can be commercially or politically motivated. However, for global data exchange, an Identity Provider is required that is accepted by as many parties as possible. To close this gap, decentralized Public-Key-Infrastructures (PKI) concepts have been introduced in the past, in which independent PKIs can trust each other and thus maximize the web of trust between the authenticated actors of each PKI [22,23].

3. **Sovereign data exchange**: In addition to the technical difficulties, there are also general reservations about the exchange of information between maritime actors. There are various reasons why companies and organizations are hesitant to share data with other parties. One of the main concerns is the fear that by sharing information, third parties may be able to obtain sensitive business data and trade secrets [24]. At a time when data are playing an increasingly important role in business success, the security and confidentiality of this information is of paramount importance. Therefore, many companies are careful when it comes to sharing their data with other actors. In order to address this issue, a data infrastructure is required that allows stakeholders to maintain full control over their data at all times and decide for themselves which stakeholders can access their own data under which conditions. In the past, a centralized solution, such as a data lake, was often used to share data. In this case, data from all participating actors were migrated to a central location and managed centrally from there [25]. However, centralized architectures have only proven themselves in the context of smaller initiatives where all participants know and trust each other. The larger the centralized infrastructure becomes, the greater the risk that the individual

actors will not trust each other and therefore not want to make their data accessible to everyone at one central location [12]. For this reason, a decentralized infrastructure is required in the global maritime domain that allows maritime actors to continue to store their data locally and only share it when necessary under conditions defined by them.

4. **Management of maritime environmental conditions**: An additional challenge in maritime data exchange is that vessels at sea often only have very limited and expensive bandwidth [26]. Furthermore, the internet connection is unstable, leading to unpredictable disconnections and therefore communication problems [27]. This represents a significant hurdle for the efficient exchange of information, as the reliability and continuity of communication is not guaranteed, meaning that it cannot be ensured that relevant information is always available if individual seaside actors have no connection to the shoreside. This in turn means that data-driven services can no longer be offered at this point, leading to economic or security-related losses. To meet this challenge, concepts and technologies are required that increase the availability of information and at the same time make it possible to deal with limited bandwidths and frequently interrupted connections. This can include the use of data compression technologies, the prioritization of important messages and the automatic recovery of data transmission in the event of connection interruptions. It is also important to minimize redundancy in data transmission, as usually only current information is of interest for traffic management and other maritime services.

2.2. Sovereign Data Exchange

The concept of Data Spaces originated from the need to share data in a world where data are gradually becoming one of the most important goods [9]. In contrast to most conventional goods; data are not consumed when used to extract higher-value information [28]. Nevertheless, as data are a valuable asset, the natural instinct is to protect them and not simply share them with others. However, a key characteristic of data is that, unlike other goods, their total added value increases when they are used as often as possible [11]. In order to derive the greatest possible benefit from the available data, barriers for the exchange of information must be reduced and transparency increased as much as possible. This is the only way to enhance the willingness of other actors to make their own data available for other purposes. Nowadays, data exchange takes place via centralized platforms that make the provider of the data vulnerable, as it does not retain full control over its data and must rely on the trustworthiness of the platform provider [29]. In addition, this results in a large number of smaller data infrastructures that are generally not interoperable. The resulting data silos make it difficult for Data Consumers and providers to exchange data with any actors outside their own silo [18]. One approach that has recently emerged as a promising solution to the challenges of ensuring data sovereignty is the concept of Data Spaces [13]. By Nagel and Lycklama Data Spaces has been defined as a "*decentralized infrastructure for trustworthy data sharing and exchange in data ecosystems based on commonly agreed principles*" [12]. In a Data Space, the individual actors are able to persist their data locally and decide for themselves under which conditions they want to exchange certain pieces of information, as well as with whom and when [30]. This means that no central instance is required to which the data have to be migrated, as is the case, e.g., when using centralized approaches such as data lakes or a data warehouses [9,11]. Information is only exchanged when required and the information access and usage policies can be defined in detail by the provider of the data by itself [9,15]. The goal is that data cannot be further used without the knowledge and permission of the data owner. In this way, the Data Provider retains full control over its data, as only it can view all access requests and approve them

according to its own requirements. As already mentioned, other centralized data management systems can be beneficial if all parties involved know and trust each other. However, since this article focuses on the maritime application of information exchange, the special characteristics of the maritime domain need to be considered as well. In the globalized maritime sector, many participants have to exchange information with each other without knowing each other beforehand. A centralized data management architecture that everyone worldwide can trust is unfeasible. Therefore, the approach of decentralization seems to be very promising to enable a trustworthy and comprehensive data exchange

In recent years, the scientific community has been working intensively on the conceptualization of Data Spaces, identifying and standardizing the relevant components and describing the interaction between the various actors in a data ecosystem [31]. One initiative that has emerged as one of the trailblazers in the area of Data Spaces is the International Data Space Association (IDSA). One of the main activities of the IDSA is the development of a Reference Architecture Model (RAM)—a blueprint for the development of Data Spaces. The intent behind the RAM is that developers of Data Spaces should adhere as closely as possible to the guidelines and principles set out in the IDSA RAM when designing and implementing their infrastructures. The IDSA RAM provides a comprehensive architecture and methodology that facilitates the creation of a secure, trustworthy and interoperable data infrastructure. By following these guidelines, developers can ensure the basic principles of data sovereignty, security and interoperability [30].

Figure 1 shows an overview of a generic Data Space architecture based on the IDSA RAM [18]. The focus of a Data Space lies always on the exchange of data between two participants (c.f. Figure 1; Data Space Participant *A* and *B*).

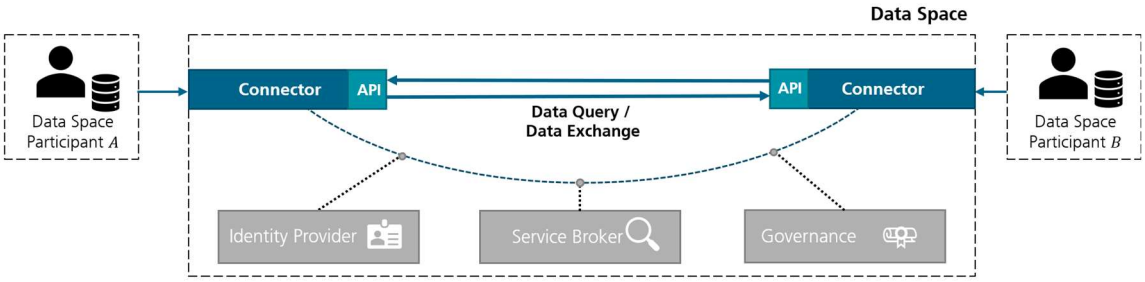

Figure 1. Architecture of a generic Data Space (based on the IDSA RAM-4 [32]).

All interactions between the individual participants in a Data Space take place via so-called Connectors. The Connectors therefore form the heart of every Data Space, as they are responsible for sending and responding all requests [18]. Every Connector within a Data Space always has a predefined set of standardized interfaces so that every Connector can be addressed exactly in the same way. This increases interoperability and reduces the barriers for data exchange. The Connector is also responsible for setting up a secure, encrypted communication channel and the authentication of Data Space Participants between each other [18,29]. Generally, each Data Space Participant provides its own Connector, which is operated on its own infrastructure, and therefore full control can be retained over the Connector. An important design pattern of Data Spaces is that only the participant's own Connector is able to directly access the data. All external data requests are received and processed by the Connector first. Direct access to the underlying data infrastructure is not possible for any Data Space Participant. The Connector evaluates the request and decides whether or not to make the requested data available to the Data Consumer's Connector. The Connector only forwards the data to the Data Consumer if the self-defined policies are adhered to. If the policies are violated, the Connector will reject the request.

In addition to the Connectors themselves, each Data Space usually has further so-called Federated Services that support the sovereign and secure exchange of data by providing additional functions within a Data Space and can be used equally by all Data Space Participants [33]. The most central Federated Services are the *Identity Provider* (for secure authentication and authorization) and the *Service Broker* (for finding services). Federated Services are usually provided by trusted actors, like companies, organization or nations. Since Federated Services are used equally by all participants throughout the Data Space, it is important that there is a transparent process in which all participants can co-determine the services used and influence all other decisions that affect the principles of the respective Data Space (e.g. audit of new applicants) [9]. Only when the participants agree on a common set of ground rules that define the shared principals of the Data Space can a foundation for trust and cooperation be established. Only transparent and joint decision-making can create trust in the principles of the Data Space and its Federated Services—trust is the entire basis for the willingness of Data Space Participants to share data with each other. This crucial role is usually carried out by a Governance body. Depending on the Data Space, all participants of a Data Space, companies, organizations or governments can usually be part of the Governance. As mentioned earlier, one of the most important Federated Services for building trust among the Data Space Participants is an Identity Provider that provides every participant with a unique identity and an associated digital certificate. With the provided identity and the associated certificate, each participant can be uniquely addressed and authenticated. The associated certificate can also be used to sign messages digitally and encrypt data transmission. In this way, it can be ensured that each participant is actually communicating with the person they intended to communicate with. In contrast, the *Service Broker* is a service that can support the participants of a Data Space in their search for relevant data sources and services. Since a Data Space is a decentralized system, finding interesting data is an enormous challenge. The *Service Broker* is usually a kind of central Yellow Pages directory in which the participants can publish their own Connectors so that they can be found by other participants. In addition, the *Service Broker* provides meta-information about the Connector and its data, which provides further information about the data offered and its endpoint, via which the data can be requested.

The Connectors, the Identity Provider, the Data Broker and Governance are the main components of (almost) every Data Space; in addition, Data Spaces can also provide other Federated Services as required, such as a standardized vocabulary to increase the interoperability of the individual data sources, an App Store for the provision of so-called Data Apps that can be executed directly within a Connector to further strengthen the sovereignty of the Data Provider or a Clearing House with which data transactions can be documented securely and traceably [9].

2.3. Requirements for a Maritime Data Management System Ensuring Secure and Reliable Data Exchange

Based on the above considerations regarding maritime traffic management and its dependence on an up-to-date database, the associated challenges in the sharing of data in the maritime sector and new approaches to the decentralized and sovereign sharing of data, the following requirements for the development of a system that enables the reliable and secure exchange of data to support maritime traffic management can be derived:

1. **Sovereign and secure data provision**: Sovereign and secure data provision is crucial for maritime actors, as it ensures that Data Providers retain full control over their own data and can independently determine who they grant access to. This not only ensures the integrity and confidentiality of sensitive maritime information, but also promotes the willingness to share data with each other.

2. **Connection of heterogeneous data sources**: A comprehensive information base (weather, logistics, ship, harbor,...) is required for the proper execution of activities in the maritime domain, which is provided by the individual actors via a wide variety of different technical interfaces (SQL, REST, FTP,...). The system must therefore be able to handle the heterogeneity of the data sources in terms of both content and technology.
3. **Integrity and certification**: For a trustworthy exchange of information, it is important that the users of the system can securely authenticate and authorize each other cryptographically and digitally sign their messages. This prevents a malicious actor from impersonating another actor. It also makes targeted attacks, such as a man-in-the-middle, more difficult.
4. **Finding data**: Due to the large number of maritime actors and available data sources and services, the system must allow users to search the available data sources using various filters so that each actor can find the data sources relevant to them depending on their individual use case.
5. **Availability of maritime data**: As maritime services are often safety-critical systems, reliable data exchange is crucial. This poses a particular challenge for communication between maritime and land-based actors due to the low bandwidth available and unexpectedly interrupted connections. The system to be developed must therefore make it possible to conserve bandwidth, handle volatile connections and enhance the availability of maritime information accordingly.

3. Related Work

This section presents a comprehensive overview of existing architectures and research activities related to Data Spaces within the maritime domain. It highlights the focus areas of these research initiatives and their respective goals. The section concludes with a differentiation of the objectives and requirements pursued in this paper.

International Data Space Association (IDSA)/GAIA-X: The International Data Spaces Association (IDSA) and GAIA-X are key initiatives in the European data economy, each playing a different but complementary role to each other. GAIA-X aims to create a comprehensive European cloud infrastructure that promotes interoperability between different cloud services and providers and creates an open market for digital services [34]. One particular focus here is on designing the market in such a way that it complies with the European values on data usage in accordance with the General Data Protection Regulation (GDPR) [35]. The focus is on the development of technical standards, governance models and best practices to ensure a secure environment for data usage [36]. In contrast, IDSA focuses specifically on the development of standards for trusted data exchange, with a focus on data ownership, sovereignty and interoperability [29]. In the literature, GAIA-X is often mentioned in the same breath as IDSA. Although the two initiatives have similar intentions, they have a different focus, which means that their defined standards complement rather than contradict each other [34]. With their defined standards and reference implementations, they provide best practices that should be considered when developing new Data Spaces. In this way, design errors can be avoided and interoperability between different Data Spaces can be further increased in order to reduce data silos.

Marispace-X: One prominent Data Space under the GAIA-X umbrella is Marispace-X, designed specifically for marine big data applications [37]. It focuses on collecting, merging, and processing data from drones, satellites, sensors and other measure instruments from the sea. The aim of Marispace-X is to simplify the sharing and processing of this information so that further services, such as munitions clearance in the North- and Baltic Sea, can be developed more efficiently and as many parties as possible can benefit from the existing

data instead of having to collect it by themselves. Marispace-X is built on the IDSA-RAM framework, supplemented by Federated Services developed by GAIA-X. The project defines five specific use cases in the maritime sector, engaging stakeholders from industry, academia, and government, to explore the potential of the Data Space. These use cases include the internet of underwater things, offshore wind energy, unexploded ordnance in oceans, biological climate protection, and critical infrastructure management [37].

DataPorts: Another related European Data Space initiative is DataPorts, developed under the HORIZON 2020 framework by the European Union. This project aims to create a secure data platform for information sharing within port communities and infrastructures [38]. The platform connects to existing digital infrastructures in participating ports and explores the application of blockchain technology in the port environment. The DataPorts platform draws inspiration from the IDSA RAM and emphasizes leveraging collected data for analytics, including AI applications, to optimize business processes. While DataPorts tackles challenges related to sovereign and secure data provision, it does not provide solutions for high-availability data exchange between maritime and terrestrial environments.

Virtual Watchtower (VWT): The Virtual Watchtower (VWT) project serves as a cross-industry collaboration tool for supply chain risk management, particularly in response to incidents like the blockage of the Suez Canal by the Ever Given in 2021 [39]. VWT aims to enhance digitalization in end-to-end cargo operations by integrating all actors in the logistics chain [40]. It focuses on data sharing from the cargo owner's perspective, enabling timely assessments of delays due to external factors, such as storms. Although VWT provides a comprehensive view of the entire supply chain, its scope is primarily geared towards logistics management rather than facilitating information exchange among maritime actors.

Maritime Data Space (MDS): The Maritime Data Space (MDS), initiated in Norway by the research foundation SINTEF, is another significant Data Space built on the IDSA-RAM. Its goal is to establish trusted data exchange between ships and shore-based entities to optimize activities of maritime actors with compliance to EU reporting requirements [11]. The architecture incorporates a Connector, service broker, and certification authority, alongside a Public Key Infrastructure (PKI). The PKI used in the MDS are the results of the CySiMS research project [41]. Although the Maritime Data Space (MDS) represents a significant milestone in the development of maritime Data Spaces to optimize maritime activities, several challenges remain. One main problem concerns the Federated Services, which are designed as centralized services. Given the global nature of the maritime domain, relying on a centralized PKI does not seem to be a viable option, as it could lead to potential bottlenecks and single points of failure. Furthermore, the availability of information from sea-based actors is only guaranteed if there is a connection between sea-based and land-based actors. The continuous availability of information at sea, especially in times without a direct connection, is currently not considered. These aspects require further consideration and development in order to improve the resilience and efficiency of maritime Data Spaces.

CISE: The CISE project, spearheaded by the European Maritime Security Agency (EMSA), aims to develop an architecture that connects existing legacy systems from various maritime surveillance entities [42] This architecture is based on so-called adaptors to link nodes established at both national and European levels, ensuring compatibility among diverse legacy systems. The subsequent EFFECTOR project extends CISE's capabilities by establishing a data lake-like structure to facilitate big data operations on collected raw data from these legacy systems [43].

In evaluating the presented projects and initiatives, it becomes evident that most of them are grounded based on the IDSA framework, which provides a robust foundation

for data governance and sovereignty, which are core concepts of any Data Space. Due to different requirements, both the VWT and CISE projects pursue a solution that differs from the IDSA. Nevertheless, what all the projects presented have in common is that in data ecosystems involving many different parties, the sovereignty of the data is of the highest importance and must be guaranteed by suitable methods such as a decentralized architecture and secure authentication and authorization. However, it is noticeable that all the initiatives presented take the availability of information as a given. This is by no means the case, especially when it comes to information from seaside actors, whose connection can be interrupted at any time. It is therefore of great importance to investigate how such decentralized systems for sovereign data exchange can be supplemented in such a way that the availability of information between maritime actors is increased as much as possible. The more up to date the available information is, the more precisely services can be developed on this basis to improve the operational activities of maritime actors.

4. Concept

As already described in the Section 2.2, the main barrier to sharing information between maritime actors is the concern that they will lose control over their own data and will no longer be able to control who has access to which data under which conditions. The architecture to be developed must therefore be structured in such a way that the sovereignty of the Data Providers is always preserved. Over the past years, Data Spaces have emerged as the foundation for the design of data management architectures in connection with the requirement for data sovereignty. With the decentralized approach, all data stocks remain persistent on the infrastructure of the Data Providers, and a central instance, as in the case of data lakes, can be avoided, so that the Data Provider continuously maintains full control over all its data [18]. Data are only exchanged between two parties when required, provided the Data Provider approves a request from a Data Consumer. Thus, the concept presented in this paper is also based on a decentralized Data Space architecture (see Figure 2).

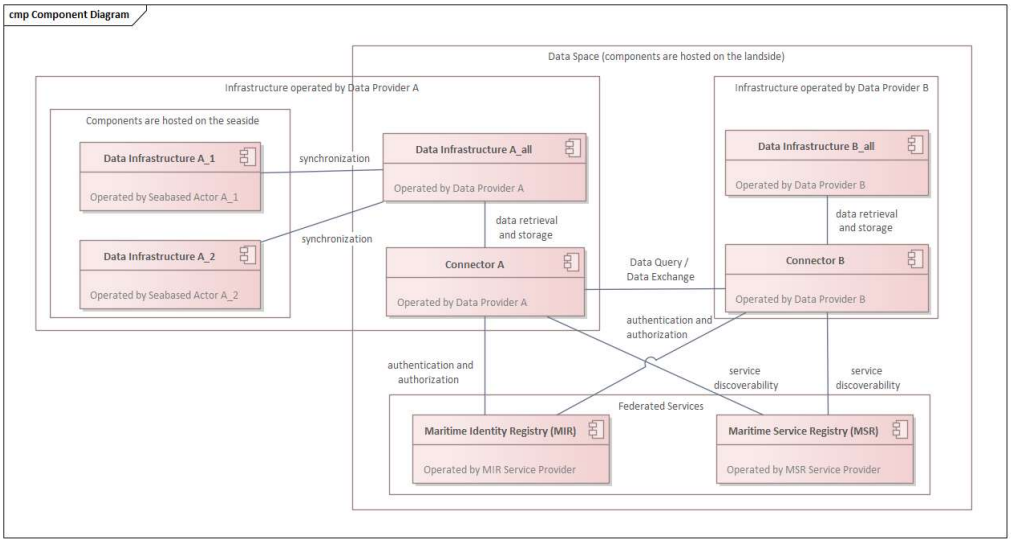

Figure 2. Overall proposed architecture for sharing data in a sovereign and secure way under consideration of maritime requirements.

Figure 2 visualizes the overall architecture of the system for the sovereign and secure exchange of data, considering the maritime requirements with their individual components and their interactions with each other. The following sections describe the functionality of the architecture and its individual components in detail. In principle, the concept can

be divided into a sea-based (left-hand side) and a land-based part (right-hand side). The proposed architecture foresees that all components of the Data Space are hosted on the land. Therefore, there are no Connectors or Federated Services on the seaside. The underlying idea is that every seaside actor (e.g., ship, wind farm, etc.) belongs to one Connector on the landside. This Connector can, for example, be hosted by a legal entity, such as the shipping company or the seaside actor itself. In this way, it is also conceivable that, e.g., a shipping company could provide the data of all its vessels via one single Connector instead of having to operate a separate Connector for each vessel. However, to be able to make the data of the seaside actors available on the landside via the Connector, the data must first find its way from the seaside to its landside infrastructure.

For this purpose, each seaside actor has its own seaside infrastructure on which data about the actor itself or its environment is recorded (see Figure 2, Data Infrastructure A_1 and A_2). The seaside data infrastructures are always linked to a landside data infrastructure (cf. Figure 2, e.g., Data Infrastructure A_{all}) on which all information available on the seaside from a Data Provider is mirrored and persisted on the landside. The data infrastructure A_{all} of Data Provider A therefore contains all data stocks of data infrastructure A_1 and A_2. In addition, the Data Provider A can also persist other information in its data infrastructure A_{all} that has not been collected by seaside actors (such as current information about the hinterland connections). Both the seaside and landside data infrastructures are usually databases in which the data can be persisted in a structured way. Overall, this setup of the architecture offers two major advantages over hosting one seaside Connector each:

Scalability: By outsourcing the Connector to the landside, all requests to the Data Provider are also processed on the landside. This has the great advantage that the information from seaside actors only needs to be mirrored once on the landside and is then available on the landside for all other Data Consumers. The data volume required between the seaside and landside is therefore reduced to a minimum. In addition, a Data Provider only has to operate one Connector in this way. If the data were not collected centrally on a data infrastructure on land, each actor (including those at sea) would have to operate their own connector in order to interact with the Data Space. Depending on the number of actors, this entails a large technical overhead that can also be greatly reduced by outsourcing the Connectors onshore.

Availability: By outsourcing the Connector and mirroring the data on the landside, information from seaside actors can also be requested by Data Consumers even if they are not currently available themselves. If a seaside actor loses its connection, the last version of information immediately before the connection loss can still be queried in this way. If the data were not mirrored on land, it would not be possible to retrieve the information in such situations. This maximizes the availability of information under consideration of volatile connections on sea.

The entire interaction between the land-based actors takes place following the standards of the International Data Spaces Association. For this purpose, the Connectors with their standardized interfaces for peer-to-peer communication are supported by additional Federated Services. According to IDSA, a minimal Data Space has at least one Identity Provider and one Service Broker [29]. In the maritime use case examined in this paper, Federated Services that have been explicitly developed for the requirements of the maritime domain should preferably be used. For this purpose, the Maritime Connectivity Platform (MCP) offers the Maritime Identity Registry (MIR) as a maritime Identity Provider and the Maritime Service Registry (MSR) as a maritime service broker [44]. Both Federated Services are based on maritime standards from the International Association of Lighthouse Authorities (IALA) and follow the International Maritime Organization (IMO) e-navigation

strategy [45]. In the following sections, we take a closer look at the individual components of the architecture presented and the processes behind them.

4.1. Maritime Federated Services

As described in Section 2.2, a crucial prerequisite for trustworthy data exchange is the possibility of secure authentication and authorization between maritime actors. A navigational warning, for example, is not credible without information about its origin. In the digital world, trust is ensured chiefly via cryptographic means, like a Public Key Infrastructure, where digital identities can be authenticated via encrypted certificates. To tackle the challenges regarding the globality and maritime regulations, Federated Services specifically developed for the maritime domain are needed. A system based on IALA guidelines is the Maritime Connectivity Platform, which provides both an Identity Provider (Maritime Identity Provider) and Service Broker (Maritime Service Registry) under the simultaneous consideration of maritime requirements. The MSR enables the exploration of maritime services provided by MCP users, and the MIR provides functionalities for authorizing and authenticating participants. Both services are challenged with the same problem of global unique identification of identities. Therefore, the Maritime Resource Names (MRN), a naming scheme, was developed by IALA to guarantee the unique identification of maritime entities. The MRN is a subspace of the Uniform Resource Name (URN) namespace and is managed by the IALA. A hierarchical structure of an MRN identifier guarantees a clear und unique identification of organizations, stakeholders, services, vessels, persons, and routes (example of an MRN: $urn : mrn : iala : aton : us : 1234.5$; the MRN describes an Aid to Navigation (AtoN) that is managed by the United States with the *id* 1234.5). Furthermore, MRNs are human-readable, which increases user-friendliness and therefore also acceptance among seafarers. Due to its explicit focus on the maritime domain, it is preferred to other Federated Service options, such as those of the IDSA itself, in this paper.

Maritime Identity Registry (MIR): The MIR is essential for trust establishment by functioning as an Identity Provider while hosting a PKI with a well-established authentication process using standards like OAuth 2.0 and OpenID Connect. Each entity that is registered in a MIR gets a certificate that is connected to its unique MRN. The concept of the MIR foresees that there is not only one single central Identity Provider, but that several Identity Providers can exist simultaneously and are interoperable with each other. For example, each individual country or harbor can provide its own MIR instance with which the registered actors can authenticate themselves. In order to prevent individual trust silos (similar to Data Spaces), policies can be formulated between the individual instances that describe whether two MIR instances trust each other or not. This creates a web of trust relationships between the individual instances so that actors who are not registered in their own MIR instance can also be trusted to be transitive. This would be the case, for example, if $MIR\ A$ trusts $MIR\ B$ and $MIR\ B$ trusts $MIR\ C$. Users of $MIR\ A$ could then still authenticate and authorize themselves with users of $MIR\ C$ (provided that a trust policy exists between $MIR\ A$ and $MIR\ C$), even if they use two different Identity Providers. This approach maximizes trust between the individual parties in a global domain, such as the maritime sector. Additionally, each MIR instance has its own MRN name-subspace, managed by the corresponding MIR itself.

Maritime Service Registry (MSR): Another challenge that arises from the global nature of the maritime domain is the finding of suitable and valuable services. It may be even challenging to find, e.g., a weather-routing service that is operated at the ship's current location. Therefore, the discovery of services has to be facilitated to minimize the effort of searching and finding services for the vessel crew or in the ship-management

office. The MCP provides such functionality for finding different services through the MSR. Maritime services can be registered and searched through a keyword or location-based search. If the search is successful, the service's endpoint and a description of how to use or consume the service can be looked up in its respective meta-information. The MSR follows the same decentralized concept as the MIR. If several MSR Service Providers trust each other, services can also be found that have not been registered in their own MSR instance.

As an example, an MCP setting is given to show how the federated structure in the MCP can be utilized to access services outside the Identity and Service Registry. In this example, there are three different MCP instances, each of which provides its own MIR. Considering the guidelines of the MCP, it is not strictly necessary that every MCP instance must provide an own MSR, but for this example we assume that each MCP instance has its own MSR. As seen in Figure 3, in our example there are in total three vessels that are registered in the following MCP instances: *Vessel* 1 is registered in instance *MCP Instance A*, *Vessel* 2 in *MCP Instance B* and *Vessel* 3 is registered in *MCP Instance A, B and C*. Additionally, in total there are three different Service Providers α, β and γ, each providing a maritime Service. *Provider* α and β are registered within *MCP Instance B*, and *Service Provider* γ is registered in *MCP Instance C*. As initially every vessel can use only the services that are registered by their own Identity Provider, *Vessel* 1 has access to no service since no service is registered in the *MCP Instance A*. However, *Vessel* 2 has access to service α and service β and *Vessel* 3 has access to service α, β and γ. As described to enhance the web of trust between maritime actors, *MCP Instances* can decide to trust each other. This in turn leads to recognizing an actor or service as trustworthy if it has been registered in the MIR or MSR of the trustworthy *MCP Instance*. In this case, *MCP Instance A* trusts *MCP Instance C* and vice versa. Through this chain of trust, *Service Provider* γ is seen as trustworthy by *MCP Instance A* and, thus, *Vessel* 1 is able to use service γ, which would be seen as not trustworthy without the mechanism of trust relationships.

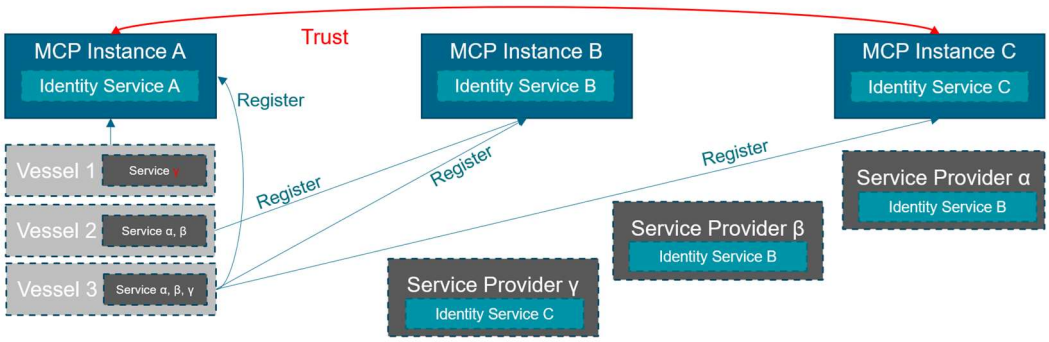

Figure 3. Overview of the federated structure of the MCP.

4.2. Connectors

In addition to the Federated Service, Connectors play a crucial role in the functionality of Data Spaces. As already outlined in Section 2, various initiatives have established standards for the development of Data Space environments. However, the defined reference architectures do not seek to define one single, universal Connector for every use case. The requirements for a Connector vary depending on the use case, which is why the establishment of a single Connector is not expedient [29]. Instead of defining one single Connector, the IDSA and GAIA-X reference architectures define a basic set of requirements for the design of Data Space Connectors with the goal to enhance interoperability and the reduction of further data silos between each other. As described in Section 3, existing Data Spaces with its Connector realizations do not yet meet all the requirements presented in this paper. Explicitly, the use of maritime identities and the increase in availability between sea

and land-based information is not yet considered in the current realizations [46]. For this reason, a personal light-weight realization of a Connector was developed, which considers both the derived standards of the IDSA RAM and further maritime standards in order to be able to meet the defined requirements in Section 2.3. To ensure security and user sovereignty, the Connector utilizes the Maritime Identity Register (MIR) for authentication and employs widely adopted security libraries for both individual data and request authorization. The developed Connector is equipped with the obligatory standardized IDSA interfaces for data consumption (*query*) and provision (*insert*) [29]. Additionally, these interfaces facilitate the seamless connection to diverse data sources, including maritime data, which is made accessible through requests and data synchronization between sea and land. In essence, this functionality is a direct proxy for maritime data sources, ensuring the availability of maritime data.

4.3. Enhancing the Avaiability of Maritime Data

In the following section, we describe the concept of how data from seaside actors can be queried by landside actors. The principle is shown schematically in Figure 4.

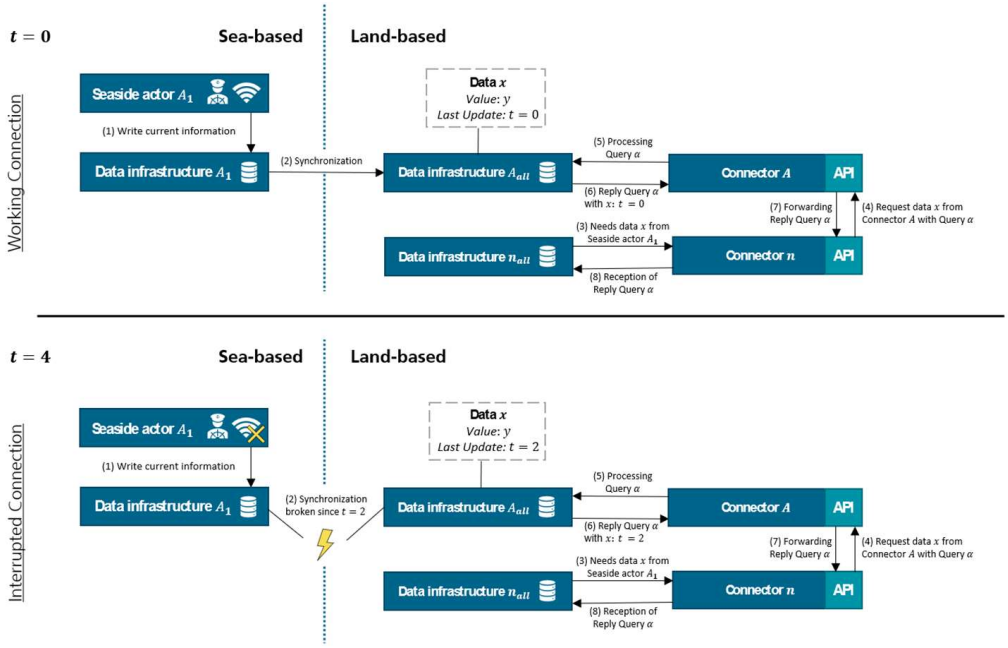

Figure 4. Querying data from seaside actors with and without an interrupted connection.

We differentiate between the state of whether the seaside actor from which information has to be retrieved is currently reachable (upper part of Figure 4) or not (lower part of Figure 4). In the upper part of the figure at time $t = 0$, the seaside actor has a stable internet connection. It therefore synchronizes its data, which is persisted locally in data infrastructure A_1 (*step 1*), to the landside in data infrastructure A_{all} (*step 2*). From there, the data can be requested by any participants of the Data Space via Connector A. Actor n requires the information x from the maritime actor A_1 (*step 3*). To obtain information x, the requester uses its own Connector n to send a query α via the standardized interfaces to the Connector of actor A (*step 4*). The request is then processed by Connector A (*step 5*). Connector A checks whether actor n is really actor n or whether someone is just trying to pretend to be actor n. Connector A is able to do that by validating the cryptographic certificate of Connector n. If the validation is successful, Connector A processes the query α and checks whether the actor n is allowed to access the data x or not.

The access rights are organized with a whitelist on which any actor must be in order to gain access to the respective data. If the actor is not on this whitelist, the query is rejected and the actor receives a message that it does not have access to the requested data. If actor n has access to the requested data, it is retrieved from data infrastructure A_{all} and forwarded to data infrastructure n_{all} via the Connectors of actor A and actor n (*step 6, 7 and 8*). It is important to note that at time $t = 0$, there was a stable internet connection between the seaside and landside and the current data was therefore constantly synchronized between data infrastructure A_1 and data infrastructure A_{all}. In this case, actor n was therefore able to retrieve the latest data from actor A_1 at time $t = 0$. The situation is different if the connection is interrupted, as can be seen in the lower part of Figure 4. In this case, for example, we are at time $t = 4$. Already at time $t = 2$, the connection from the seaside actor A_1 has been lost. Synchronization of the current information is therefore not possible for the seaside actor A_1 anymore as it has no connection to the landside. The synchronization of data has only taken place up to time $t = 2$. This means that the data infrastructure A_{all} has all the data from actor A_1 up to time $t = 2$. The data request from actor n takes place in the same way when the connection is interrupted as when the connection is stable, as the entire interaction between the Connectors in the concept has been outsourced to the landside. In this case, actor n therefore also requests data x using query α. To do this, it sends the query via its Connector n to Connector A. The latter processes the query again and, if authentication and authorization are successful, the most recent entry from date x is returned to Connector n via Connector A. In this case, the current date would be from time $t = 2$, as the synchronization of data infrastructure A_1 and data infrastructure A_{all} is interrupted since then.

The major advantage of this architecture is the increased scalability and availability of information. Due to the constant onshore mirroring of information from seaside actors, the data are not only available to other actors when the seaside actor itself is available, but also when it is not reachable. In this case, the requesting actor no longer receives the most current information, but information always has a lifespan that varies depending on the use case. This means that every actor still has the option of requesting the latest available information on a seaside actor and deciding for themselves whether or not they want to use the received data based on how current it is. In addition, any information from the seaside actors only needs to be transmitted once to the landside. This is a major advantage, especially in view of the still expensive and low bandwidth at sea. The more frequently the seaside information is requested by shoreside actors, the greater the positive contribution of the shoreside outsourcing.

4.4. Message Management During Interrupted Connections

If the connection between the seaside and landside infrastructure is interrupted, the seaside actors must have a suitable mechanism in place to organize the data that is generated during the interruption of the connection. A connection interruption can last up to several days, so that without a suitable system, a large amount of data would accumulate, which would then all have to be synchronized in an unordered way when the connection is re-established again. This procedure would not only be inefficient, as outdated information might also be transferred in this way, but it would also endanger safety, as critical information might not be synchronized first so that they might be synchronized late or even not synchronized in the event of another unexpected disconnection.

To overcome this issue, it is important to develop a suitable protocol that specifies when information is going to be transmitted. The functionality of the proposed management system is shown schematically in Figure 5. A virtual queue is introduced in order to organize the data arising in the event of a connection loss, in which the data to be transferred is successively transferred once the connection has been re-established again. An entry in the queue is made up of a sextuple $a = (actor, attribute, value, timestamp, priority, version)$, where *actor* is the MRN identifier of the actor that generates the information, *attribute* describes the type of information, *value* is the actual data of the attribute, *timestamp* specifies when the value of the attribute was recorded, *priority* indicates the priority with which the date is to be synchronized to the landside, and *version* is a counter that prevents collisions while synchronizing the messages.

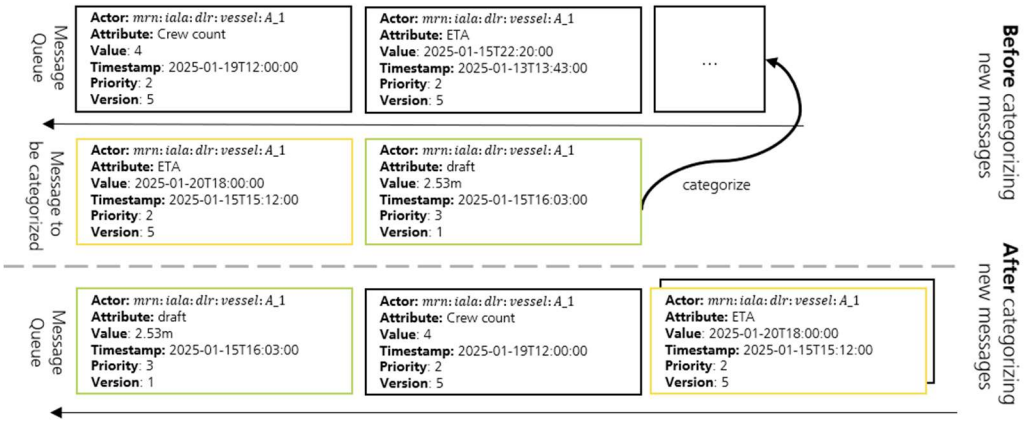

Figure 5. Virtual waiting queue during interrupted connections.

Prioritization: Due to the fact that bandwidth is very limited and volatile, it is important that safety-critical and important information can be prioritized for transmission. In practice, the operator of the sea- and landside infrastructure (see Figure 2 , actor A) will decide for all its belonging maritime actors ($here$, A_1 and A_2) which data should be prioritized for transmission. As this can vary significantly depending on the use case, we will not define a specific recommendation for the prioritization of messages in this paper. Since the operator of the seaside and landside infrastructure has its own interest in receiving the relevant information as quickly as possible and has control over all its seaside actors, there is no conflict of interest in the prioritization of the individual messages, as in a scenario with several independent actors who all want to synchronize their own messages first and therefore all send their messages with the highest priority, thus undermining the prioritization system. A simple numerical value, p , where $p \in [0 \dots m]$ is suitable as a prioritization number, has a higher value that is associated with a higher priority. Depending on the use case, a different range of priorities can be required, which is why the value m is not specified further. In the schematic example in Figure 5, the entry $m = (mrn : iala : dlr : vessel : A\_1,\ draft, 2.53,\ 2025-01-15T16:03:00,\ 3,\ 1)$ is placed at the front of the queue as the entry has a higher priority than all other messages in the queue.

Update: Prioritization helps to ensure that the most relevant information is synchronized first after a connection is established. However, information can also lose relevance during the duration of a connection loss. This is the case if the same date, e.g., the ETA of a vessel, is updated and the older value is therefore no longer relevant for most use cases. Considering the need to reduce the required bandwidth as much as possible, synchronizing the outdated information would not be beneficial. Instead, the entry with the outdated value will be overwritten with the new value so that there is a maximum of one entry in

the queue at the same time for each attribute of an actor. This applies to the entry $n = (mrn : iala : dlr : vessel : A\_1,\ ETA, 2025-01-15T22:20:00, 2025-01-13T13:43:00, 2, 5)$ of the vessel A_1, where the ETA is updated from "2025-01-15T22:20:00" to "2025-01-20T18:00:00". However, the new message $k = (mrn : iala : dlr : vessel : A\_1,\ ETA,$ 2025-01-20T18:00:00, 2025-01-15T15:12:00, 2, 5) takes the place of n in the queue. This has the advantage that outdated information is not transferred and only the most recent entry needs to be mirrored to the landside.

4.5. Synchronization of Message Queues to Landside Infrastructure

The question that remains is how to mirror the entries from the waiting queue to the landside infrastructure without causing conflicts during synchronization. Conflicts can arise, for example, if several maritime actors want to update the same date in the central database. In this paper, we propose two ways in which an infrastructure operator can deal with this challenge.

Consistency per seaside actor: The first and simplest option is to avoid write conflicts by allowing each seaside actor to completely mirror its own data to the landside infrastructure. In this way, if several seaside actors would like to update the same data attribute, a separate entry would be persisted on the landside infrastructure for each seaside actor with the value perceived by the respective actor. The advantage of this approach is that no write conflicts need to be resolved, as each seaside actor has its own write area on the landside infrastructure in which it can synchronize its data. The main disadvantage of this solution is that there may now be several entries for the same attribute. If the value of an attribute will be queried, several entries could be returned in this case and the requester would therefore first have to individually assess which message to trust.

Consistency per land-side infrastructure: Another option is to keep only one valid entry per land-side infrastructure. For the synchronization of messages in the maritime domain, the so-called *optimistic replication* is suitable, in which it is not necessarily assumed that the information basis of all actors is consistent with each other at all times. Optimistic replication is used, for example, in Version Control Systems (VCS). Especially when synchronizing data between sea- and land-based actors, a constant connection is not guaranteed. In order to ensure that the individual systems remain operational even if the connection is interrupted, optimistic replication is suitable, as no constant synchronization between the actors is required, as would be the case with pessimistic replication. However, the challenge when using optimistic replication is that several actors can process the same message independently of each other, meaning that conflicts can arise while synchronization with the landside infrastructure takes place. These conflicts must first be resolved before the message can be updated on the landside infrastructure. In order to be able to reliably identify whether a planned update would result in a conflict or not, optimistic replication uses a versioning for each of their messages. For example, both actors A_1 and A_2 may want to update the same data attribute x on the landside infrastructure A_{all}. Both actor A_1 and A_2 have persisted the same version of data attribute x locally from the seaside infrastructure. Now, we assume that the connection is broken for both actors and, despite the lost connection, they are still allowed to edit their local copy of data attribute x. To do this, the attribute value of the sextuple is updated and the version is increased by the value of 1. As soon as one of those actors, e.g., A_2, has re-established a connection, the version number of the updated message is compared with the version number of the message in the landside database. As the version number of the updated entry is 1 higher than the version number of the entry in the landside infrastructure, the entry in the shoreside database is overwritten with the entry from A_2. As soon as the other actor, here A_1, also re-establishes its connection and wants to synchronize its updated data, it will notice that the version

number of its own entry is the same as the entry in the landside infrastructure. In this case, a conflict arises because the entry has been updated based on an outdated version. In such a case, the conflict must be resolved before the entry from A_1 can be synchronized to the landside infrastructure. In the maritime use case, for example, the timeliness of an entry is suitable for resolving the conflict so that the more recent message overwrites the older message. However, other approaches are also feasible, such as entries from authorities being classified as more valuable and therefore overwriting information from supposedly less credible actors.

5. Application and Evaluation

Given the broad range of potential applications for the proposed system, we illustrate several use cases using the example of a system for optimizing maritime traffic, operated by a Vessel Traffic Service as an evaluation.

5.1. Introduction to Case Study

A Vessel Traffic Service (VTS) would like to use a Traffic Management System (TMS) to improve the coordination of vessels entering the port. On the basis of a range of information, the TMS derives recommendations for action for the individual traffic participants, which optimize maritime traffic in terms of waiting times in the roadstead and emissions. However, the TMS relies on data about the current traffic situation, such as information about the position, speed, ETA, unexpected delays, weather information and information from the port about available services, such as pilots, moorings, cranes and connections to the hinterland. To derive recommendations for action, the coordination problem is first modeled mathematically and then solved using genetic algorithms. When deriving the recommendations, the TMS concentrates on adjusting the speed of the individual traffic participants so that they receive a prompt from the system to increase or reduce their current speed accordingly. For reasons of practicability, the TMS does not adjust the route or other parameters. In macroscopic terms, following the recommendations for action leads to an optimization of the overall traffic situation. The solution generated by the TMS is robust to the extent that ignoring individual recommendations for action does not directly cause the solution as a whole to collapse. However, the current traffic situation is continuously monitored by the TMS with regard to increasing efficiency. If the system detects that too many traffic participants are not following the recommendations for action or that other environmental conditions, such as the available port services, have changed unexpectedly, the TMS automatically generates a new solution that takes the deviating environmental parameters into account when finding a solution. As already mentioned, the TMS is only able to derive recommendations for action for the traffic participants if it also has access to the required heterogeneous data basis. The aim of the case study is to show how the data management system from Section 4 can support the operational provision of data-driven services using an exemplary service for optimized traffic coordination. For this purpose, the concrete evaluation scenario is first described below, before the functionality of the prototype is then explained on the basis of three defined user stories.

5.2. Evaluation Scenario: Traffic Management Optimization Problem

To illustrate how the presented concept actually works, we will focus on a simple traffic management optimization problem with only one traffic participant that is to be solved by the TMS. The evaluation scenario comprises a total of three actors who are dependent on exchanging data with each other in order to optimize the traffic situation (c.f. Figure 6).

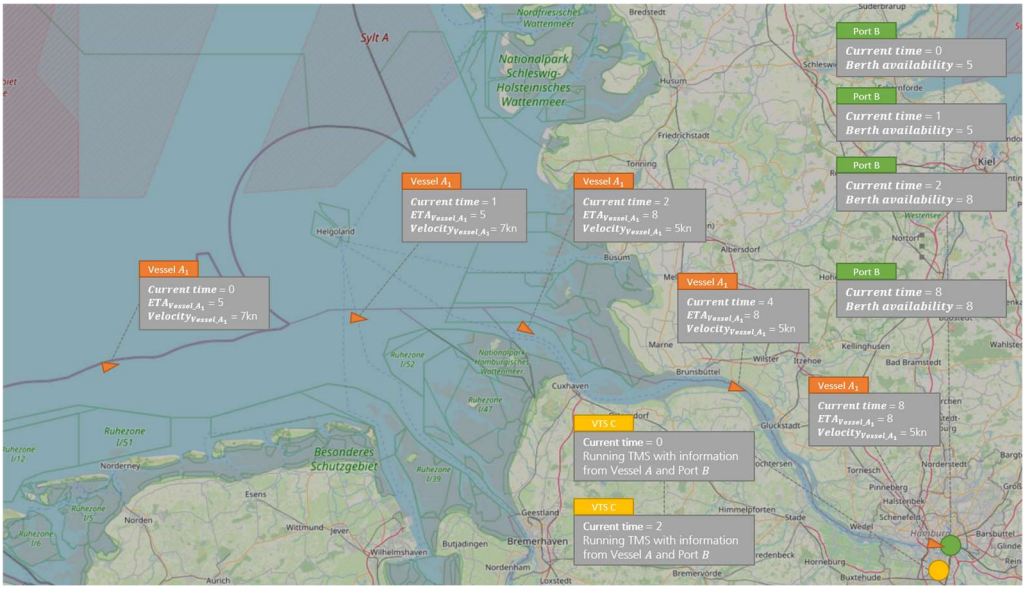

Figure 6. Exemplary traffic optimization scenario.

The actors are *Shipping Company A*, which has up-to-date information about its *Vessel* A_1, *Port B*, with its port-related information, and *VTS C*, which ultimately wants to optimize traffic by operating the TMS. The simple scenario assumes that the incoming *Vessel* A_1 wants to enter the Elbe estuary at a speed of 7 *knots* at time $t = 0$, so that it will enter the port at time $t = 5$ as agreed with the port. At time $t = 2$, however, there is an unexpected delay in the port, so that the berth intended for *Vessel* A_1 will not be available at time $t = 5$. The planned berthing time for *Vessel* A_1 is therefore adjusted by *Port B* to time $t = 8$. *VTS C* would now like to optimize the current traffic situation in order to ensure that *Vessel* A_1 arrives at the port just in time and that there arise as few waiting times as possible. For this purpose, *VTS C* uses the TMS, which can derive how *Vessel* A_1 must adjust its speed based on the current position of *Vessel* A_1 and the available berths of *Port B* in order to enter the port without waiting time. Based on the current position of *Vessel* A_1 and the time of the next available berths in *Port B*, the service suggests reducing the speed of the vessel to 5 *knots*. The recommended action is communicated by *VTS C* to *Shipping Company A* so that the vessel adjusts its speed accordingly and can enter *Port B* at time $t = 8$ without waiting. The prerequisite for deriving the recommendations for action from the TMS is that the *VTS C* can access the information from *Shipping Company A* and *Port B*. For this purpose, the data management system architecture presented in this paper is used to enable secure and sovereign data exchange between these actors. Based on the acquired data, the *VTS C* can then operate its data-driven TMS service, as described, for traffic optimization.

5.3. Setup for Provision of Required Data Basis

To operate the TMS, *VTS C*, as described in 6.2, requires access to the data about the ETA and velocity of *Vessel* A_1 and the current port utilization of *Port B*. The information is distributed across a total of two parties—namely, *Shipping Company A* and *Port B*. In accordance with the concept from Section 4, all actors use a Data Space Connector for uniform and sovereign data exchange, which is connected to their own data infrastructure (see Figure 7). *Shipping Company A* collects data from its seaside *Vessel* A_1, which is why data are synchronized from Data Infrastructure A_1 to Data A_{all} in accordance with the concept presented in Section 4.3. Therefore, there is no direct data exchange between *Vessel* A_1 and *VTS C*. Instead, the *VTS C* obtains the required information via the Connector from

Shipping Company A. To increase the global discoverability and secure authentication and authorization of the data exchange, the Connectors are supported by the Maritime Service Registry and Maritime Identity Registry. For the evaluation, the traffic data of *Vessel* A_1 and the entire current traffic situation are simulated by the Maritime Traffic Simulation (MTS) of the German Aerospace Center. The MTS makes it possible to realistically simulate entire traffic situations with a large number of vessels using ship type-dependent physic models and intelligent vessel behavior. The MTS generates Automatic Identification System (AIS) and radar messages in NMEA0183 format as output, which serve as a basis for the validation and verification of maritime systems. In the following, the functionality of the developed architecture will be shown based on the described setup, which demonstrates how (a) data can be found and queried, (b) the data can be exchanged in a sovereign and secure way, and (c) the provision of information can be guaranteed even in the case of instable connections at sea.

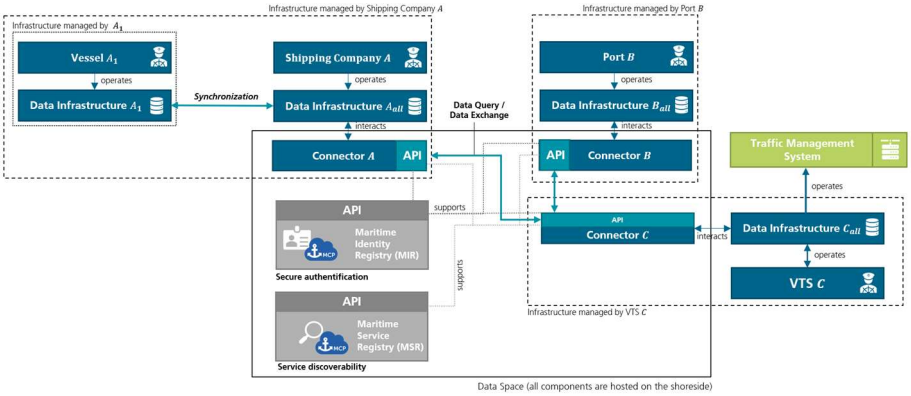

Figure 7. Evaluation setup for validating the functionality of the data space architecture.

5.4. Finding Nessacary Data

The Maritime Service Registry is used as a broker to find the required information. All services (and therefore also Connectors) can be registered by the service providers in the MSR in accordance with IALA Guideline G1128. If a potential service consumer is looking for specific data, the MSR can be used as a first point of contact to find suitable Connectors (c.f. Section 2.3, R4, finding data). For this purpose, users can use an API provided by the MSR or a graphical user interface in which they can formulate structured queries. In this way, the user can search the registered services with regard to various attributes such as name, MRN, geographical coverage and status (see Figure 8).

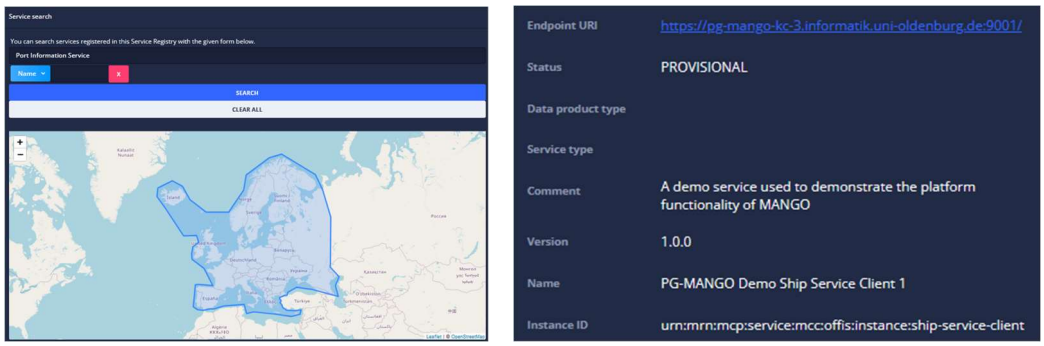

Figure 8. Search for suitable Connectors in the Maritime Service Registry (**left**: data Consumer is looking for a service that provides data about the ports in Europe; **right**: as a return, it receives a connector with the necessary meta-information and an endpoint that can be addressed for obtaining the requested information).

If the user decides on a service, they can display further meta-information and the endpoint of the service so that the user is subsequently able to address the service itself directly. It is crucial that as many Connectors as possible that should be publicly discoverable are also registered in the MSR so that the widest possible coverage of services can be found using the MSR. In the presented architecture, the use of the MSR should only be regarded as optional; if the Data Consumer already knows a suitable Data Provider and its endpoint, the search in the MSR can be skipped. In the presented case study, the VTS C uses the MSR to find a source that has information about Vessel A_1. The MSR suggests the Connector from *Shipping Company A* to the VTS C for this purpose. The source for the other data required to operate the TMS is already known to the VTS C (Connector from Port B). The VTS C therefore does not need to request any further information about Port B from the MSR.

5.5. Souvern and Secure Data Sharing

Due to the decentralized nature of the architecture presented, data can also be used to provide data-driven services without the need to migrate your own databases to a central infrastructure. The Data Providers can continue to persist their heterogeneous data on their local data infrastructure (see Figure 7, Data Infrastructure A_{all}, B_{all}, C_{all}) and can only provide the data requested by a Data Consumer via their Connector if required (c.f. Section 2.3, R2) Connection of heterogeneous data sources). In the evaluation scenario, the VTS C requires information about Vessel A_1 and the existing port services of Port B to operate its TMS service. The VTS C formulates one data request to Shipping Company A and another request to Port B to query the required information basis. In this way, both Data Providers receive a request for their data from VTS C and can decide individually whether they want to provide the requested information to VTS C or not. In contrast to a central data infrastructure, they therefore always retain full control over access to their data (c.f. Section 2.3, R1, sovereign and secure data provision). The access rights are realized via a whitelist of the respective Connector. All data requests and data exchanges take place entirely via the standardized Connectors and their uniform interfaces (see Figure 9). In this way, a request is possible even if, for example, Shipping Company A enters Port B for the first time and is completely unknown to VTS C. Thanks to the standardized Connectors, they can still exchange information with each other in a uniform way without having to align their IT-infrastructures beforehand. The central interfaces of the Connector are the *insert*- and *query*-API. The interfaces are aligned to the IDSA RAM 4.0. With the *insert*-API, new or updated data can be made available to Data Consumers via their own Connector. A total of three parameters are required for this: *serviceMRN* specifies the MRN of your own Connector via which the data to be entered is made available; the *dataPath* specifies a JSON path behind which the data to be entered is stored in the Connector; priority is an optional parameter with which the Data Provider can configure the relevance of the date. The priority parameter is mainly used for the synchronization of messages between sea and land.

In the evaluation scenario, Port B wants to update its current berth availability at time $t = 2$ and therefore calls the insert-API. The exemplary call is shown in Figure 10, left. The port with the MRN "urn : mrn : iala : mcp : port : B" updates its berth availability, which is located behind the JSON path "$.*services.berths.steinwerder.berth_availability*", with the value 8 and transmits it with a priority of 0. The VTS C then queries the updated data independently using the *query*-API in order to consider the value during the traffic coordination. For a valid query, the *query*-API requires the serviceMRN of the Connector to be accessed and the dataPath that refers to the date to be requested. The VTS C can derive

both from the MSR and the meta-information provided. The request made by the VTS C is shown in Figure 10 on the right.

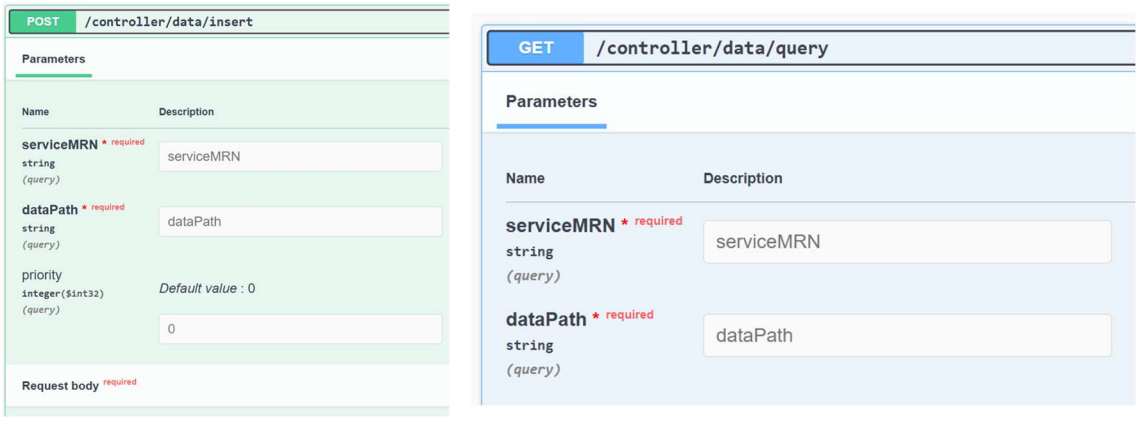

Figure 9. Standardized Connector APIs (**left**: providing data via the insert API; **right**: request data via the query API).

Figure 10. Exemplary call of the port's Insert API to update its berth availability.

The VTS C asks the Connector " urn : mrn : iala : mcp : port : b " for its value, which is hidden behind the attribute "$.berths.steinwerder.berth_availability". The Connector of PortB processes the received request and uses the whitelist to check whether the VTSC has access to the data attribute or not. The VTSC has access to the date and receives the updated value 8 in response, which it then utilized for the operation of the TMS. The VTSC also sends a corresponding query request to the Connector of Shipping Company A in order to receive current information about Vessel A_1.

All communication between the Connectors is encrypted using the X.509 certificates issued by the Maritime Identity Registry. By using the MIR certificates, the actors can securely authenticate each other cryptographically and thus ensure that they are communicating with the intended actor (c.f. Section 2.3, R3, integrity and certification). Encryption and authentication significantly reduce the risk of the message exchange being read or even manipulated by unwanted third parties.

5.6. Continuous Provision of Required Data

During the provision of information, Vessel A_1 experiences an unexpected connection loss at time $t = 1$, so that it is no longer possible to establish an IP-based communication with the vessel. However, according to the architecture presented, the vessel had already migrated its data from its local Data Infrastructure A_1 to the shore-side infrastructure of its Shipping Company A_{all} at time $t = 0$. In this situation, no up-to-date values can be retrieved from the vessel at time $t = 1$, but at least any information at the time of the last synchronization $t = 0$ can still be accessed. The VTS C therefore still has the option at time $t = 1$ to request the Connector from Shipping Company A and thus retrieve the information from Vessel A_1 at time $t = 0$ and be able to further operate its TMS based on the available information basis (c.f. Section 2.3, R5, availability of maritime data). Since

all information is always requested and exchanged via the shore-side infrastructure, the break-even point with regard to the required seaside data volume is already reached with the first request for a date (see Figure 11). Each further request leads to a linear reduction in data volume as the number of requests increases. Only if a date is not requested at all are more data exchanged between the data infrastructures.

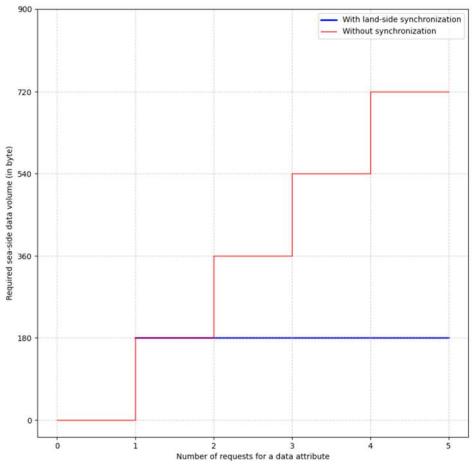

Figure 11. Required seaside data volume depending on the number of data requests.

During the disconnection, Vessel A_1 can continue to update its attributes locally. To do this, it follows the protocol written in Section 4 in which only the most recent value for an attribute is persisted in the waiting queue. Older values are overwritten and not synchronized in order to reduce the total band volume required (see Figure 12).

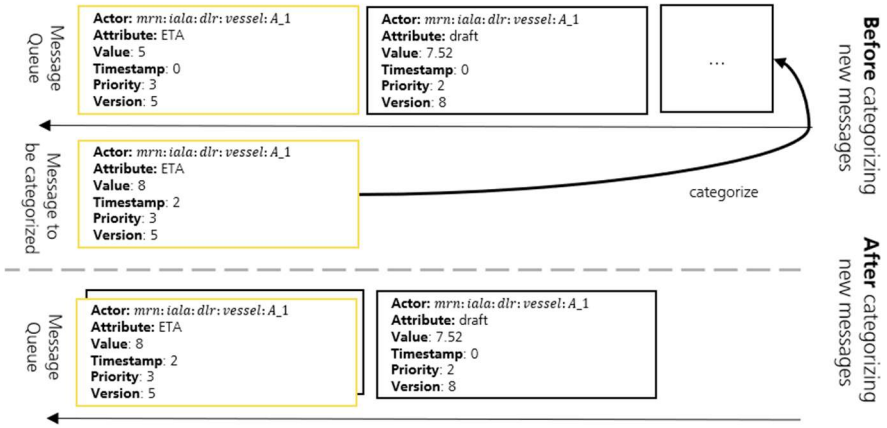

Figure 12. Classification of new data in the queue.

When the internet connection is re-established, the queue of Vessel A_1 is then synchronized to the shore-sided Infrastructure A_{all}. During the transfer of the queue, a check is made to see whether any synchronization conflicts will occur when updating the shore-side values. Shipping Company A synchronizes its data according to the described principle of "Consistency per land-side infrastructure", where there is only one valid value for each date, regardless of the source from which it originates. Therefore, when updating the planned ETA of Vessel A_1, the version number of the message from the queue must be compared with the version number in the Data Infrastructure A_{all}. If the version number of the message is 1 higher than the existing version number of the message in the data infrastructure A_all, the message was not updated by any other actor during the disconnection. In this case, there is no conflict and the message can be transferred to Data Infrastructure A_{all}.

6. Discussion

In summary, the applicability of the presented system was demonstrated using a typical use case from the field of maritime traffic management. With the Traffic Management System, it was possible to show how a data-driven service can be supplied with the necessary information to support the efficiency and safety of maritime traffic using the decentralized data infrastructure presented in this paper. In addition, the presented architecture meets the requirements derived in Section 2.3 for a data infrastructure to ensure sovereign and secure maritime data exchange while taking volatile connectivity into account:

1. **Sovereign and secure data provision:** Due to the fully-decentralized architecture of the data infrastructure, the sovereignty of the individual Data Providers remains protected. The information of the individual Data Providers remains continuously stored on their infrastructure and is only transmitted to potential Data Consumers when required. Furthermore, a Data Consumer cannot access the data source of a Data Provider directly at any time. Instead, all requests and information are always exchanged and transmitted via a Connector—which represents a further level of security. Additionally, Data Providers can decide for themselves using a whitelist which data should be made available to which Data Consumer under which conditions.
2. **Connection of heterogeneous data sources:** Additionally, the proposed architecture enables uniform access to the heterogeneous data sources of the various Data Providers through the use of standardized Connectors. Regardless of the underlying technology of the data source, the Data Providers offer their data via the *insert*-API of the Connector provided for this purpose. In addition, all data requests are sent to the standardized *query*-API (c.f. Section 4.2.). The work for the mapping between the interfaces of the Connectors and the underlying technology of the data source, such as (SQL, REST, FTP,. . .) is the responsibility of the operator of the Connector itself. However, the mapping enables any further interaction with the Data Space components and their actors to be completely standardized and no further adjustments to the respective IT infrastructures need to be made. In this way, data can also be exchanged spontaneously in critical situations, for example, even between two unknown parties. A one-off exchange of information would also be possible in this way, which would otherwise not be economically viable due to the potentially high level of adaptation work required for the infrastructures.
3. **Integrity and certification:** By using the Maritime Identity Registry of the Maritime Connectivity Platform, the actors involved can authenticate each other securely with the digital identities issued by the MIR and transmit the messages to be exchanged in encrypted form. This is a critical prerequisite for creating trust in the data management architecture so that the participants in the Data Space can securely verify who they are communicating with. Only if the participants can authenticate each other can it be ensured that the data are really forwarded to the intended actor and that no one can impersonate another actor. Due to the decentralized approach of the MIR and the consideration of maritime standards, such as the use of MRNs as identities, trust among the participants is maximized by the resulting web of trust compared to the use of a central Identity Provider.
4. **Finding data:** The optional use of the Maritime Service Registry, on the other hand, allows users to search the data space for relevant data sources based on various parameters. This makes it easier to find suitable data sources for a wide variety of use cases. For a more detailed assessment of the data source, meta-information and the endpoint for querying the Connector are also provided.

5. **Availability of maritime data**: Last but not least, the architecture also includes measures that are automatically carried out in the event of a disconnection from a sea-sided actor. The synchronization protocol presented here ensures that only the most up-to-date information is transmitted in order to conserve the required data volume. The prioritization option ensures that the most critical information is synchronized first and can be made available to the Data Consumers. Land-side data mirroring maximizes the availability of sea-side information. Even in the event of an interrupted connection of a seaside actor, the latest version can still be retrieved onshore at any time. In addition, any data requests for seaside actors are answered by the landside. As can be seen in Figure 11, this leads to a break-even point in terms of the total required data volume per attribute with a single request. Each additional request leads directly to a reduction in the total required seaside data volume. However, it should be noted that even if information is not requested, the one-off synchronization of the date on the land side results in costs that would not be caused by a direct sea-side query. The volume of data required for synchronization is heavily dependent on the update frequency of the individual attributes. The more frequently the sea-side attributes are updated, the more frequently a message is exchanged between the sea-side and shore-side infrastructure, which in turn contributes to an increase in the needed data volume. However, this is the inevitable consequence for the constant availability of seaside information on land. In addition, the required data volume can be further reduced by an intelligent update frequency. Using the approaches presented in Section 4.5 to maintain consistency between the seaside and landside infrastructure (Consistency per seaside actor and Consistency per landside infrastructure), conflicts can be resolved even if several actors want to update the same attribute independently of each other.

In contrast to previous work in the field of maritime data management, which has been presented in Section 3 and compared with respect to the fulfillment of the requirements derived in Section 2, the presented architecture fully addresses the relevant requirements for a data management system for the secure and sovereign provision of information. Although, there are already approaches in the literature that support individual necessary aspects, such as the sovereign sharing of information, the connection of heterogeneous data sources and the reliable retrieval of distributed data (e.g., Marispace-X, DataPorts, Maritime Data Space). Other relevant aspects, such as increasing the availability of sea-based information and the use of maritime standards and existing Maritime Federated Services, have not been fully integrated in any of the previous work (c.f. Section 3). This implies that the architecture presented in this paper complements the current state of the art in two respects:

(1) On the one hand, the paper supplements the concept of Data Spaces with an approach for the constant availability of information from seaside actors, which is of central importance for the reliable provision of maritime value-added services. The approach of mirroring the information on land and the associated permanent availability allows for information about the latest status of a seagoing actor to be provided even if a connection to the actor itself is not possible at the current time. This is particularly important for the advancing digitalization of the maritime domain, as many maritime services are dependent on the constant availability of information, including that of seaside actors, as shown by the evaluation scenario from Maritime Traffic Management.

(2) On the other hand, the concept for the overall architecture was developed with a particular focus on maritime standards. Already established maritime solutions were applied as Federated Services, so that components from the Maritime Connectivity

Platform were used for the secure authentication and authorization of maritime actors and the discovery of services. MRNs were also used as identifiers to address actors. This demonstrates how current standardization efforts in the maritime domain can be applied in a practical use case in the field of maritime data management and create an added value for maritime stakeholders by using services and protocols that actively address maritime needs.

7. Conclusions

In this paper, we discussed the need for a data management system that fulfills the requirements for data-driven services to support maritime operational activities. Based on the current literature, we first identified the research gap discussed in this paper and formulated requirements for a corresponding maritime data management system. On this basis, a system architecture was derived that considers the interests of the actors involved in the exchange of maritime data and addresses challenges such as unpredictable disconnections and low bandwidth. The architecture is based on a decentralized Data Space structure in order to preserve the sovereignty of the actors. In addition, concepts have been integrated that increase the availability of information between sea and land and at the same time reduce the data volume that is required on the seaside. A practical case study demonstrated its functionality based on a maritime traffic management scenario. The presented architecture closes the research gap for a data management concept that allows maritime actors to securely exchange their data without compromising their sovereignty. The concept also explicitly addresses the challenges posed by the involvement of sea-side actors and maximizes data availability to support the provision data-driven services. In summary, the proposed architecture represents a holistic approach for a data management system in the maritime domain that enables maritime actors to securely and sovereignly exchange data with each other despite low available bandwidth and unexpected connection losses in order to reliably operate their data-driven services.

Limitations and Future Work

Nevertheless, some limitations of the current architecture should be mentioned, which can be further investigated in future research:

Compliance with further standards: The architecture presented in this paper initially focuses on the use of standards from the maritime domain (such as IALA G1128, G1161, R1023, among others) in order to first gain acceptance in the maritime community. Not considering maritime standards would doom the proposed data management system to fail, even in the context of smaller use cases, as many already deployed systems are based on these standards and would therefore be incompatible with the proposed architecture. Nevertheless, in future, it would be desirable to take a closer look at the standards of ongoing Data Space initiatives. However, a major challenge in the simultaneous consideration of maritime standards and the guidelines of established Data Space initiatives, such as GAIA-X and the IDSA, lies in their partial contradictions. In an initial analysis, some contradictions were already identified between the maritime standards and the IDSA RAM, for example, in the formats used for identifiers (e.g., MRNs in the maritime domain and Universally Unique Identifier (UUID) in the IDSA RAM). In order to ensure conformity with the standards of both domains, the concept would have to be expanded to include further IDSA standards and a corresponding compromise would have to be found for every event of contradictions. In many cases, these contradictions can be resolved by a matching approach, e.g., between MRNs and UUIDs. Conformity between the standards of both domains would be desirable in principle, as it could increase interoperability with other related Data Spaces and prevent data silos.

Serialization to reduce data volume: In addition to increasing conformity with existing standards, the size of the exchanged messages could be further reduced from a technical perspective, by using suitable serialization methods to reduce the size of each single message. Approaches that do not transmit the schema directly in the payload of each individual message, such as ProtoBuff, are particularly suitable for this. In this way, the actors involved would only have to send the schema of a message to each other once. For each transmitted message, the payload of the message is then combined with the schema once transmitted. Especially for smaller messages, the schema of a message can make up a large part of the payload, which can be further reduced using suitable serialization methods.

Data Apps to enhance data sovereignty: Furthermore, additional protection of the sovereignty of Data Providers could be achieved by extending the Connectors to include the principle of Data Apps, in which the data-driven services must be executed directly in the Connector itself instead of outside. This means that the requested data can only be used for the operation of the respective service, so that the Data Consumer can also operate its data-driven service without insight into the data provided by the Data Provider and thus only has access to the higher-value information generated by its own data service, but not to the data of the Data Provider itself. The concept of Data Apps means that the Data Provider's data can be more strongly protected if required, as the Data Provider can define and control exactly for which Data Apps its data should actually be used for.

It should be noted that the success of such a decentralized infrastructure depends largely on acceptance and active use within the maritime community. The more authorities and the maritime industry decide in favor of such an infrastructure, the greater the resulting benefits for all parties involved. Although the infrastructure can also be used in smaller data ecosystems, the resulting benefits increase with a growing number of users [47]. The network effect that occurs here can be explained by the fact that actors will only use the data infrastructure in the long term if they can reliably access, find and obtain the relevant data. If the supply of available data is too low, usage will also decline over time. However, Data Providers will only offer their data via the infrastructure if sufficient Data Consumers are available. Due to the circular causality, it is all the more important that standardization bodies and authorities initiate obligatory guidelines for a standardized data exchange in the maritime domain. The efforts to date, such as the IALA G1161 or the IMO's e-navigation strategy, have already created a good foundation for the digitalization of the maritime domain. Now it is time to continue building on this in order to establish a sovereign and secure data exchange for the reliable use of maritime services.

Author Contributions: Conceptualization, D.H., C.T., B.R., L.M. and A.H.; data curation, D.H., B.R. and L.M.; investigation, D.H., C.T., B.R. and L.M.; methodology, D.H., C.T., B.R. and L.M.; project administration, D.H.; software, D.H., L.M.; supervision, A.H.; validation, D.H. and L.M.; visualization, D.H., L.M. and B.R.; writing—original draft, D.H., C.T., B.R. and L.M.; writing—review and editing, D.H., C.T., B.R., L.M. and A.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work has received funding from European Union's HORIZON research and innovation program under the Grant Agreement no. 101138583 and the Future Ports project of the German Aerospace Center (DLR).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; nor in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

AIS	Automatic Identification System
AtoN	Aid to navigation
EMSA	European Maritime Safety Agency
ETA	Estimated time of arrival
GDPR	General Data Protection Regulation
IALA	International Association of Lighthouse Authorities
IDSA	International Data Spaces
IMO	International Maritime Organization
MCP	Maritime Connectivity Platform
MDS	Maritime Data Space
MIR	Maritime Identity Registry
MRN	Maritime Resource Name
MSR	Maritime Service Registry
MTS	Maritime Traffic Simulation
PKI	Public-Key-Infrastructure
RAM	Reference Architecture Model
TMS	Traffic Management Service
URN	Uniform Resource Name
UUID	Universally Unique Identifier
VCS	Version control system
VTS	Vessel Traffic Service
VWT	Virtual Watch Tower

References

1. Shone, R.; Glazebrook, K.; Zografos, K.G. Applications of stochastic modeling in air traffic management: Methods, challenges and opportunities for solving air traffic problems under uncertainty. *Eur. J. Oper. Res.* **2021**, *292*, 1–26. [CrossRef]
2. IMO. Just in Time Arrival Guide. GloMEEP Project Coordination Unit, 2020. Available online: https://greenvoyage2050.imo.org/wp-content/uploads/2021/01/GIA-just-in-time-hires.pdf (accessed on 1 April 2025).
3. Van Westrenen, F.; Praetorius, G. Maritime traffic management: A need for central coordination? *Cogn. Technol. Work* **2014**, *16*, 59–70. [CrossRef]
4. Greidanus, H.; Alvarez, M.; Eriksen, T.; Gammieri, V. Completeness and Accuracy of a Wide-Area Maritime Situational Picture based on Automatic Ship Reporting Systems. *J. Navig.* **2016**, *69*, 156–168. [CrossRef]
5. El Mekkaoui, S.; Benabbou, L.; Caron, S.; Berrado, A. Deep Learning-Based Ship Speed Prediction for Intelligent Maritime Traffic Management. *J. Mar. Sci. Eng.* **2023**, *11*, 191. [CrossRef]
6. Pahl, J. Just-in-Time Port Call Optimization: Challenges and IT-Systems. *J. Phys. Conf. Ser.* **2024**, *2867*, 012009. [CrossRef]
7. Praetorius, G.; Hollnagel, E. Control and Resilience Within the Maritime Traffic Management Domain. *J. Cogn. Eng. Decis. Mak.* **2014**, *8*, 303–317. [CrossRef]
8. GrgičEvi, L.; Coates, E.M.L.; Fossen, T.I.; Bye, R.T.; Osen, O.L. Centralised Decision Support in Maritime Vessel Traffic Services: A Polymatrix Game Solution. 2025. Available online: https://www.researchgate.net/publication/388218361_Centralised_Decision_Support_in_Maritime_Vessel_Traffic_Services_A_Polymatrix_Game_Solution (accessed on 1 April 2025).
9. Lind, M.; Hägg, M.; Siwe, U.; Haraldson, S. Sea Traffic Management—Beneficial for all Maritime Stakeholders. *Transp. Res. Procedia* **2016**, *14*, 183–192. [CrossRef]
10. Xiao, Z.; Fu, X.; Zhao, L.; Zhang, L.; Teo, T.K.; Li, N.; Zhang, W.; Qin, Z. Next-Generation Vessel Traffic Services Systems—From "Passive" to "Proactive". *IEEE Intell. Transport. Syst. Mag.* **2023**, *15*, 363–377. [CrossRef]
11. von Zernichow, B.M.; Nesheim, D.A. Maritime Data Space (MDS) Final Project Report. SINTEF Digital, June 30, 2021. Available online: https://www.sintef.no/projectweb/maritime-data-space-mds/results/ (accessed on 4 June 2024).

12. Nagel, L.; Lycklama, D. *Design Principles for Data Spaces—Position Paper*; International Data Spaces Association: Berlin, Germany, 2021. [CrossRef]
13. Aslam, S.; Michaelides, M.P.; Herodotou, H. Internet of Ships: A Survey on Architectures, Emerging Applications, and Challenges. *IEEE Internet Things J.* **2020**, *7*, 9714–9727. [CrossRef]
14. Inmarsat. Inmarsat FleetBroadband Service Plans. Available online: https://web.archive.org/web/20241223000710/https://satellitephonestore.com/fleetbroadband-service (accessed on 6 February 2025).
15. Iridium and Europa Satellite. Iridium Data Plans: Uninterrupted Global Connectivity. Available online: https://www.europasatellite.com/de-eu/Iridium-Openport-Airtime-s/2186.htm (accessed on 6 February 2025).
16. Inmarsat. Enterprise Services Comparison: A Quick Reference Guide. 2020. Available online: https://web.archive.org/web/20201017004229/https://www.inmarsat.com/wp-content/uploads/2014/06/Enterprise-services-May-2014.pdf (accessed on 1 April 2025).
17. Figueiredo, A.S. Data Sharing: Convert Challenges into Opportunities. *Front. Public Health* **2017**, *5*, 327. [CrossRef]
18. *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage*; Otto, B., Ten Hompel, M., Wrobel, S., Eds.; Springer: Cham, Switzerland, 2022; ISBN 978-3-030-93975-5.
19. Voelsen, D. Maritime kritische Infrastrukturen: Strategische Bedeutung und geeignete Schutzmaßnahmen. *SWP-Studie* **2024**. [CrossRef]
20. Jankowski, D.; Möller, J.; Wiards, H.; Hahn, A. Decentralized Documentation of Maritime Traffic Incidents to Support Conflict Resolution. *J. Mar. Sci. Eng.* **2022**, *10*, 2011. [CrossRef]
21. Albarqi, A.; Alzaid, E.; Ghamdi, F.A.; Asiri, S.; Kar, J. Public Key Infrastructure: A Survey. *J. Inf. Secur.* **2015**, *6*, 31–37. [CrossRef]
22. Bhattacharjee, R.M.B.; Katz, J.; Marsh, M. KeyChains: A Decentralized Public-Key Infrastructure. Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7704be9a5f57fe4c82414ae11211e44440591a4d (accessed on 1 April 2025).
23. MCC Identity Management and Security: General Approach and Basic Requirements, MCP IDsec 1. Available online: https://maritimeconnectivity.net/wp-content/uploads/2023/02/MCP-Concept-v2.pdf (accessed on 1 April 2025).
24. Curry, E. *Real-Time Linked Dataspaces: Enabling Data Ecosystems for Intelligent Systems*; Springer International Publishing: Cham, Switzerland, 2020; ISBN 978-3-030-29664-3.
25. Nargesian, F.; Zhu, E.; Miller, R.J.; Pu, K.Q.; Arocena, P.C. Data lake management: Challenges and opportunities. *Proc. VLDB Endow.* **2019**, *12*, 1986–1989. [CrossRef]
26. Jensen, R.B. Fragmented digital connectivity and security at sea. *arXiv* **2020**. [CrossRef]
27. Alqurashi, F.S.; Trichili, A.; Saeed, N.; Ooi, B.S.; Alouini, M.-S. Maritime Communications: A Survey on Enabling Technologies, Opportunities, and Challenges. *arXiv* **2022**. [CrossRef]
28. Ramge, T.; Mayer-Schönberger, V. *Machtmaschinen, 2. Auflage*; Murmann: Hamburg, Germany, 2020; ISBN 978-3-86774-651-9.
29. International Data Spaces Association. IDS Reference Architecture Model 4. 2022. Available online: https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4 (accessed on 22 April 2024).
30. Jarke, M.; Otto, B.; Ram, S. Data Sovereignty and Data Space Ecosystems. *Bus. Inf. Syst. Eng.* **2019**, *61*, 549–550. [CrossRef]
31. Curry, E.; Scerri, S.; Tuikka, T. (Eds.) *Data Spaces: Design, Deployment and Future Directions*; Springer: Cham, Switzerland, 2022; ISBN 978-3-030-98636-0.
32. Franklin, M.; Halevy, A.; Maier, D. From databases to dataspaces: A new abstraction for information management. *SIGMOD Rec.* **2005**, *34*, 27–33. [CrossRef]
33. Siska, V.; Karagiannis, V.; Drobics, M. *Whitepaper Building a Dataspace: Technical Overview*; Austrian Institute of Technology GmbH: Vienna, Austria, 2023.
34. Braud, A.; Fromentoux, G.; Radier, B.; Le Grand, O. The Road to European Digital Sovereignty with Gaia-X and IDSA. *IEEE Netw.* **2021**, *35*, 4–5. [CrossRef]
35. Ganter, C. Gaia-X Introduces the Compliance Document to Enable and Increase Trust, Security, and European Sovereignty in Digital Ecosystems. *Press Release GAIA-X*, Sepetember 2024. Available online: https://gaia-x.eu/news-press/gaia-x-introduces-the-compliance-document-to-enable-and-increase-trust-security-and-european-sovereignty-in-digital-ecosystems/ (accessed on 1 April 2025).
36. BMWi. GAIA-X: Technical Architecture. July 2020. 2025. Available online: https://www.bmwi.de/Redaktion/EN/Publikationen/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=6 (accessed on 1 April 2025).
37. Wehner, D.; Dell, S.; Neumann, A.J.; Wendt, J. MARISPACE-X: Digitalizing the ocean—The future of maritime data in the European federated data infrastructure GAIA-X. *Int. Hydrogr. Rev.* **2022**, *28*, 76–93. [CrossRef]
38. DataPorts. DataPorts—Platform Architecture and Specifications. Available online: https://dataports-project.eu/wp-content/uploads/2022/02/DataPorts_D2_4_Platform_Architecture_and_Specifications_pu_v1_2_final.pdf (accessed on 1 April 2025).
39. Fan, S.; Yang, Z.; Wang, J.; Marsland, J. Shipping accident analysis in restricted waters: Lesson from the Suez Canal blockage in 2021. *Ocean Eng.* **2022**, *266*, 113119. [CrossRef]

40. Virtual Watch Tower—OnePager. November 2023. Available online: https://virtualwatchtower.org/wp-content/uploads/2023/11/VWT_One-pager_ver-2023-11-12.pdf (accessed on 28 May 2024).
41. Bernsmed, K.; Bour, G.; Meland, P.H.; Borgaonkar, R.; Wille, E. CySiMS-SE Deliverable. SINTEF Digital, March 25, 2021. Available online: https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/3018532/D4.3+Multi-modal+communication.pdf?sequence=1 (accessed on 1 April 2025).
42. Rajamäki, J.; Tikanmäki, I.; Räsänen, J. CISE as a Tool for Sharing Sensitive Cyber Information in Maritime Domain. *Inf. Secur. Int. J.* **2019**, *43*, 215–235. [CrossRef]
43. Kapidani, N.; Astyakopoulos, A.; Bolakis, C.; Moutzouris, M.; Hajduch, G.; Vosinakis, G.; Scrima, P.; Paladin, Z. Maritime information sharing environment deployment using the advanced multilayered Data Lake capabilities: Effector project case study. *Pomorstvo* **2022**, *36*, 291–304. [CrossRef]
44. IALA. G1161—Evaluation of Platforms for the Provision of Maritime Services in the Context of E-Navigation. June 2021. Available online: https://www.iala.int/product/g1161-evaluation-of-platforms-for-the-provision-of-maritime-services-in-the-context-of-e-navigation/ (accessed on 10 February 2025).
45. International Maritime Organization. Strategy for the Development and Implementation of E-Navigation. 2006. Available online: https://wwwcdn.imo.org/localresources/en/OurWork/Safety/Documents/enavigation/MSC%2085%20-%20annex%2020%20-%20Strategy%20for%20the%20development%20and%20implementation%20of%20e-nav.pdf (accessed on 1 April 2025).
46. International Data Spaces Association. Data Connector Report. Available online: https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-Data-Connector-Report-84-No-16-September-2024-1.pdf (accessed on 1 April 2025).
47. Möller, F.; Jussen, I.; Springer, V.; Gieß, A.; Schweihoff, J.C.; Gelhaar, J.; Otto, B. Industrial data ecosystems and data spaces. *Electron. Mark.* **2024**, *34*, 41. [CrossRef]